Claims

What I claim as my invention is:

1. A system for maintaining a digital-imaging file, comprising:

computer means having installed therein a trusted time source;

means for saving the file at a moment in time;

API means for selectively retrieving from said trusted time source a date and a time corresponding to said moment in time;

means for appending said date and said time retrieved from said trusted time source to said saved file; and

means for saving said file with said certificate appended thereto.

2. The system according to claim 1, further comprising:

means for signing said saved file with said date and said time retrieved from said trusted time source appended thereto;

means for hashing said signed file to produce a digest;

means for signing said digest with a key to produce a certificate; and

means for appending said certificate to said saved file.

3. The system according to claim 1, further comprising means for verifying the authenticity of said file with said certificate appended thereto.

4. The system according to claim 3, wherein said verification means comprises means for signing said saved file with said date and said time retrieved from said trusted time source appended thereto with an ID.

5. The system according to claim 4, wherein said ID is selected from the group consisting of an ID corresponding to a user, an ID corresponding to a system used by said user, and an ID corresponding to an enterprise within which said user uses the system.

6. The system according to claim 5, wherein said ID corresponding to a system used by said user is elected from the group consisting of a platform ID, a server node ID, and a network ID.

7. The system according to claim 5, wherein said user ID is selected from the group consisting of a plurality of characters identifying said user, first data representing an iris scan of said user, second data representing a retina scan of said user, third data representing a finger scan of said user, fourth data representing said user's hand geometry, fifth data representing said user's voice, sixth data representing said user's signature, and combinations of said plurality of characters, first, second, third, fourth, fifth, and sixth data.

8. The system according to claim 1, wherein said trusted time source comprises:

a real time clock; and

a battery coupled to and powering said real time clock.

9. A method of maintaining a digital-imaging file in computing means, comprising:

providing a trusted time source in the computing means;

saving the file at a moment in time;

selectively retrieving from said trusted time source a date and a time corresponding to said moment in time;

appending said date and said time retrieved from said trusted time source to said saved file; and

saving said file with said certificate appended thereto.

10. The method according to claim 9, wherein said computing means further comprises a system clock, operating system means for operating the computing means, and an application running on the operating system means, and said step of selectively retrieving from said trusted time source further comprises the step of providing an API between the trusted time source and the application, wherein said API is adapted to select a date and a time from the system clock in a first plurality of instances, and to select said trusted time source a date and a time corresponding to said moment in time in a second plurality of instances.

11. The method according to claim 10, further comprising the steps of:

signing said saved file with said date and said time retrieved from said trusted time source appended thereto;

hashing said signed file to produce a digest;

signing said digest with a key to produce a certificate; and

appending said certificate to said saved file.

12. The method according to claim 10, wherein said first plurality of instances comprise a first plurality of operating system calls which are unrelated to the application.

13. The method according to claim 10, wherein said second plurality of instances comprise:

a second plurality of operating system calls, each of which relates to the application; and

a plurality of application calls which are unrelated to the operating system means.

14. The method according to claim 10, further comprising the step of providing tamper-evident means for labeling said trusted time source.

15. The method according to claim 10, wherein said moment in time corresponds to an access of the digital-imaging file.

16. The method according to claim 10, wherein said moment in time corresponds to a creation of the digital-imaging file.

17. The method according to claim 10, wherein said moment in time corresponds to a modification of the digital-imaging file.

18. The method according to claim 10, wherein said moment in time corresponds to a receipt of the digital-imaging file.

19. The method according to claim 10, wherein said moment in time corresponds to a saving of the digital-imaging file.

20. The method according to claim 10, wherein said moment in time corresponds to a transmission of the digital-imaging file.

21. The method according to claim 10, wherein said step of providing an API between the trusted time source and the application further comprises the step of preventing changes to the system clock.